(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－328033

(43)公開日　平成11年(1999)11月30日

(51)Int.Cl.[6]		識別記号	FI		
G06F	12/14	320	G06F	12/14	320A
	17/60		G09C	1/00	660D
G09C	1/00	660	G06F	15/21	Z

審査請求　未請求　請求項の数7　ＯＬ　（全 13 頁）

(21)出願番号　特願平10－138663

(22)出願日　平成10年(1998)５月20日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　内海　研一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　平野　秀幸
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

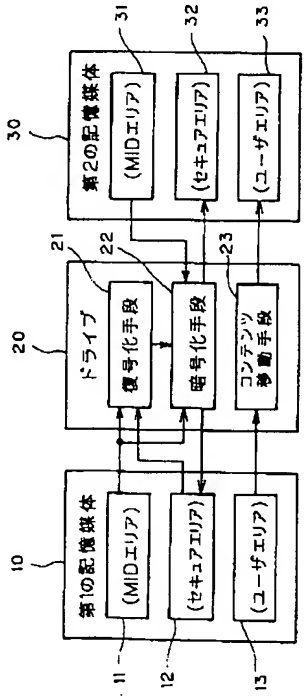
(74)代理人　弁理士　山田　正紀

(54)【発明の名称】　ライセンス委譲装置

(57)【要約】

【課題】本発明は、コンテンツの使用権を委譲するライセンス委譲システムに関し、そのコンテンツに関し権利を有する者の保護を図りつつ、そのコンテンツの複製や頒布等を行なう。

【解決手段】鍵１でコンテンツを暗号化し、その鍵１および使用権情報４１を、それらが格納された記憶媒体１０を特定するメディアＩＤからなる鍵２で暗号化しておき、そのコンテンツの使用権を委譲するにあたり、コンテンツは鍵１で暗号化された状態のまま、委譲先の記憶媒体３０に移し、鍵１および使用権情報４１を移転前の記憶媒体１０のメディアＩＤで復号化し、さらに委譲先の記憶媒体３０のメディアＩＤで暗号化して、委譲先の記憶媒体３０に格納する。



1

【特許請求の範囲】

【請求項１】　所定の鍵により暗号化されたコンテンツと、自分を特定する第１のメディアＩＤと、前記鍵と該コンテンツの使用権を表す第１の使用権情報との双方が一緒あるいは別々に前記第１のメディアＩＤで暗号化されてなる第１の暗号化セキュア情報とが格納された第１の記憶媒体と、自分を特定する第２のメディアＩＤが格納された第２の記憶媒体とをアクセスして前記第１の記憶媒体に格納されたコンテンツの使用権を前記第１の記憶媒体から前記第２の記憶媒体に委譲するライセンス委譲装置において、

前記コンテンツの使用権の委譲にあたり前記第１の記憶媒体に格納された第１の暗号化セキュア情報を前記第１のメディアＩＤを用いて復号化することにより前記鍵と前記第１の使用権情報とを得る復号化手段、および前記復号化手段による復号化により得られた鍵と、前記復号化手段による復号化により得られた第１の使用権情報があらわす第１の使用権が譲渡あるいは分与された第２の使用権をあらわす第２の使用権情報との双方を一緒にあるいは別々に前記第２のメディアＩＤで暗号化することにより第２の暗号化セキュア情報を生成して前記第２の記憶媒体に格納させる暗号化手段を備えたことを特徴とするライセンス委譲装置。

【請求項２】　前記暗号化手段が、さらに、前記第１の使用権から前記第２の使用権を差し引いた後の第３の使用権をあらわす第３の使用権情報を、あるいは前記鍵と該第３の使用権情報との双方を、前記第１のメディアＩＤで暗号化して前記第１の記憶媒体に書き戻すことにより、該第１の記憶媒体に、前記第１の暗号化セキュア情報に代えて、前記鍵と前記第３の使用権情報との双方が該第１のメディアＩＤで暗号化されてなる第３の暗号化メディア情報を格納させるものであることを特徴とする請求項１記載のライセンス委譲装置。

【請求項３】　前記第１の記憶媒体が持つ前記コンテンツの使用権全体を前記第２の記憶媒体に委譲する場合に、前記暗号化手段が、前記復号化手段による復号化により得られた鍵と、前記第１の使用権の全てを受け継いだ第２の使用権をあらわす第２の使用権情報とが暗号化されてなる第２の暗号化セキュア情報を生成して前記第２の記憶媒体に格納させるとともに、前記第１の記憶媒体に格納されている前記第１の暗号化セキュア情報を構成する前記鍵を破壊させるものであることを特徴とする請求項１記載のライセンス委譲装置。

【請求項４】　コンテンツの使用権委譲前において、前記第１の記憶媒体が、暗号化された、使用権を委譲しようとするコンテンツが格納されたものであって、

コンテンツの使用権の委譲にあたり、前記第１の記憶媒体に格納された、委譲対象の暗号化されたコンテンツを読み出して、暗号化された状態のまま、前記第２の記憶媒体に格納するコンテンツ移動手段を備えたことを特徴

2

とする請求項１記載のライセンス委譲装置。

【請求項５】　前記第１の使用権情報および前記第２の使用権情報が使用権が存在することをあらわすものであり、前記第３の使用権情報が使用権が存在しないことをあらわすものであることを特徴とする請求項１記載のライセンス委譲装置。

【請求項６】　前記第１の使用権情報が、第１の使用可能回数あるいは使用可能時間をあらわすものであり、前記第２の使用権情報が、該第１の使用可能回数あるいは使用可能時間以内の第２の使用可能回数あるいは使用可能時間をあらわすものであり、前記第３の使用権情報が、該第１の使用可能回数あるいは使用可能時間から該第２の使用可能回数あるいは使用可能時間を差し引いた後の第３の使用可能回数あるいは使用可能時間をあらわすものであることを特徴とする請求項１記載のライセンス委譲装置。

【請求項７】　前記第１の記憶媒体および前記第２の記憶媒体をそれぞれ駆動する第１のドライブおよび第２のドライブを備えるとともに、該第１のドライブおよび該第２のドライブが、前記第１の記憶媒体および前記第２の記憶媒体それぞれをアクセスする、それぞれ第１のファームウェアおよび第２のファームウェアを備えたものであり、

前記復号化手段および前記暗号化手段が、前記第１のファームウェアと前記第２のファームウェアとの複合体としてのファームウェア内に構成されたものであって、

前記第１のファームウェアのみが前記第１のドライブにより駆動される前記第１の記憶媒体をアクセスする権原を有するとともに、前記第２のファームウェアのみが前記第２のドライブにより駆動される第２の記憶媒体をアクセスする権原を有するものであることを特徴とする請求項１記載のライセンス委譲装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツの使用権を第１の記憶媒体から第２の記憶媒体に委譲するライセンス委譲装置に関する。

【０００２】

【従来の技術】近年、如何にして著作権の保護の実効を図るかが問題となってきている。例えば本のような有形物の場合、頒布すること自体は複製を伴なわず、本を転売すればその本は購入者の手もとに渡り販売者のもとには本は存在しなくなり、したがって著作権の保護は比較的簡単であるが、ディジタル情報化された著作物の場合、例えばそのディジタル化された著作物をネットワークを介して送信すると自分側と相手側との双方に同じ著作物が発生し、頒布すること自体が複製を伴う結果となり、通常、このようなディジタル情報化された著作物に対する著作権の実効的な保護は極めて難しいとされている。

【０００３】
【発明が解決しようとする課題】本発明は、上記事情に鑑み、ディジタル化された文書、映画、プログラム等のコンテンツの使用権を、そのコンテンツに関し権利を有する者の保護を図りつつ委譲することのできるライセンス委譲装置を提供することを目的とする。
【０００４】
【課題を解決するための手段】上記目的を達成する本発明のライセンス委譲装置は、所定の鍵により暗号化されたコンテンツと、自分を特定する第１のメディアＩＤと、上記鍵とそのコンテンツの使用権を表す第１の使用情報との双方が一緒あるいは別々に第１のメディアＩＤで暗号化されてなる第１の暗号化セキュア情報とが格納された第１の記憶媒体と、自分を特定する第２のメディアＩＤが格納された第２の記憶媒体とをアクセスして第１の記憶媒体に格納されたコンテンツの使用権を第１の記憶媒体から第２の記憶媒体に委譲するライセンス委譲装置において、コンテンツの使用権の委譲にあたり第１の記憶媒体に格納された第１の暗号化セキュア情報を第１のメディアＩＤを用いて復号化することにより上記鍵と上記第１の使用権情報とを得る復号化手段、および上記復号化手段による復号化により得られた鍵と、および上記復号化手段による復号化により得られた第１の使用権情報があらわす第１の使用権が譲渡あるいは分与された第２の使用権をあらわす第２の使用権情報との双方を一緒にあるいは別々に上記第２のメディアＩＤで暗号化することにより第２の暗号化セキュア情報を生成して第２の記憶媒体に格納させる暗号化手段を備えたことを特徴とする。
【０００５】ここで、上記本発明のライセンス委譲装置において、上記暗号化手段は、さらに、上記第１の使用権から上記第２の使用権を差し引いた後の第３の使用権をあらわす第３の使用権情報を、あるいは鍵と上記第３の使用権情報との双方を、上記第１のメディアＩＤで暗号化して第１の記憶媒体に書き戻すことにより、第１の記憶媒体に、上記記第１の暗号化セキュア情報に代えて、上記鍵と上記第３の使用権情報との双方が第１のメディアＩＤで暗号化されてなる第３の暗号化メディア情報を格納させるものであってもよく、あるいは、第１の記憶媒体が持つ上記コンテンツの使用権全体を第２の記憶媒体に委譲する場合に、上記暗号化手段は、上記復号化手段による復号化により得られた鍵と、上記第１の使用権の全てを受け継いだ第２の使用権をあらわす第２の使用権情報とが暗号化されてなる第２の暗号化セキュア情報を生成して第２の記憶媒体に格納させるとともに、第１の記憶媒体に格納されている第１の暗号化セキュア情報を構成する鍵を破壊させるものであってもよい。
【０００６】尚、上記の、「鍵と、……第１の使用権情報との双方が一緒にあるいは別々に第１のメディアＩＤで暗号化されてなる第１の暗号化セキュア情報」は、鍵を第１のメディアＩＤで暗号化し、これとは別に第１の使用権情報を第１のメディア情報で暗号化し、それらの暗号化された鍵と暗号化された第１の使用権情報とを合わせたものを第１の暗号化セキュア情報と称してもよく、あるいは、鍵と第１の使用権情報との双方を連ねたものを第１のメディア情報で暗号化し、その暗号化された情報を第１の暗号化セキュア情報と称してもよいことを意味している。
【０００７】また、上記の、「鍵と、……第２の使用権情報の双方を一緒にあるいは別々に……第２のメディアＩＤで暗号化することにより第２の暗号化セキュア情報を生成して……」や「鍵と、……第３の使用権情報との双方が第１のメディアＩＤで暗号化されてなる第３の暗号化セキュア情報」も同様である。さらに、上記の、「第３の使用権情報を、あるいは……鍵と……第３の使用権情報との双方を、……第１のメディアＩＤで暗号化して……」は、鍵と、第１の使用権情報あるいは第２の使用権情報を別々に暗号化するシステムにおいては、第３の使用権情報のみを暗号化すればよく、鍵と第１（あるいは第２）の使用権情報を連ねたものを暗号化するシステムにおいては、鍵と第３の使用権情報との双方を連ねたものを暗号化することを意味している。
【０００８】本発明のライセンス委譲装置は、例えばＭＯ（光磁気ディスク）やハードディスクには、それぞれに固有のＩＤ（メディアＩＤと称する）が付されている点に着目し、完成されたものである。所定の鍵で暗号化されたコンテンツを流通させることによりその暗号化されたコンテンツ自体はその鍵を用いて復号化しない限り使用不可能である。そこで、その暗号化されたコンテンツを復号化するための鍵と、使用権情報（例えばそのコンテンツの使用が許可されているか否かという情報など）との双方を、その記憶媒体独自のメディアＩＤで暗号化しておく。こうすることにより、その暗号化されたコンテンツは、そのコンテンツがもともと格納された記憶媒体を離れてそれ自体が頒布されても使用不能であり、鍵もそのまま頒布したのでは頒布を受けた先ではメディアＩＤが異なるため鍵を復号化することはできず、したがって使用権のない者による無断使用が防止できる。
【０００９】このようなシステムにおいて、自分（第１の記憶媒体）の使用権を委譲先（第２の記憶媒体）に譲り渡すには、自分（第１の記憶媒体）のメディアＩＤで鍵および自分の使用権情報を復号化し、自分の使用権の範囲（例えば使用可能な残存回数）の中で使用権を分与し（あるいはその使用権全体であってもよい）、鍵と、その分与されたあるいは全体としての使用権情報を、委譲先（第２の記憶媒体）のメディアＩＤ（第２のメディアＩＤ）で暗号化してその委譲先（第２の記憶媒体）に格納させる。自分（第１の記憶媒体）には、残りの使用権（使用権が存在しないという使用権を含む）を自分

（第１の記憶媒体）のメディアＩＤ（第１のメディアＩＤ）で暗号化して自分（第１の記憶媒体）に書き戻す。あるいは使用権の全部を委譲する場合は、自分（第１の記憶媒体）では、残りの使用権（この場合は使用権が存在しないという使用権）を暗号化して書き戻す代わりに、自分（第１の記憶媒体）に暗号化された形式で格納されている鍵を破壊してしまってもよい。こうすることにより、そのコンテンツに関し権利を有する者の権利を犯すことなく使用権の譲渡が可能となる。

【００１０】ここで、上記本発明のライセンス委譲装置は、コンテンツの使用権委譲前において、第１の記憶媒体が、暗号化された、使用権を委譲しようとするコンテンツが格納されたものであって、コンテンツの使用権の委譲にあたり、第１の記憶媒体に格納された、委譲対象の暗号化されたコンテンツを読み出して、暗号化された状態のまま、第２の記憶媒体に格納するコンテンツ移動手段を備えることが好ましい。

【００１１】コンテンツ自体は暗号化された状態のまま頒布されるので、いつ頒布してもよく、例えば既に頒布されているときは鍵と使用権のみを渡せばよいが、例えば上記のコンテンツ移動手段を備えて、コンテンツの使用権の委譲にあたりそのコンテンツを第１の記憶媒体から第２の記憶媒体に移動（複製）してもよい。また、上記本発明のライセンス委譲装置において、上記第１の使用権情報および上記第２の使用権情報が使用権が存在することをあらわすものであり、上記第３の使用権情報が使用権が存在しないことをあらわすものであってもよく、あるいは、上記第１の使用権情報が、第１の使用可能回数あるいは使用可能時間をあらわすものであり、上記第２の使用権情報が、その第１の使用可能回数あるいは使用可能時間以内の第２の使用可能回数あるいは使用可能時間をあらわすものであり、上記第３の使用権情報が、第１の使用可能回数あるいは使用可能時間から第２の使用可能回数あるいは使用可能時間を差し引いた後の第３の使用可能回数あるいは使用可能時間をあらわすものであってもよい。

【００１２】このほか、例えば使用権を有する人を特定するＩＤを使用権情報としてもよく、使用権情報は、使用権の有無や範囲をあらわす情報であればどのような情報であってもよい。また、上記本発明のライセンス委譲装置において、第１の記憶媒体および第２の記憶媒体をそれぞれ駆動する第１のドライブおよび第２のドライブを備えるとともに、第１のドライブおよび第２のドライブが、第１の記憶媒体および第２の記憶媒体それぞれをアクセスする、それぞれ第１のファームウェアおよび第２のファームウェアを備えたものであり、上記復号化手段および上記暗号化手段が、上記第１のファームウェアと上記第２のファームウェアとの複合体としてのファームウェア内に構成されたものであって、上記第１のファームウェアのみが第１のドライブにより駆動される第１の記憶媒体をアクセスする権原を有するとともに、上記第２のファームウェアのみが第２のドライブにより駆動される第２の記憶媒体をアクセスする権原を有するものであることが好ましい。

【００１３】ここで、「第１のファームウェアのみが……第１の記憶媒体をアクセスする権原を有する」、「第２のファームウェアのみが……第２の記憶媒体をアクセスする権原を有する」は、例えばアプリケーションプログラム等からは、それら第１のファームウェアや第２のファームウェアを介在させずに直接には第１の記憶媒体や第２の記憶媒体をアクセスすることはできないように構成されていることを意味し、このような構成を備えると以下のような場合を含め、コンテンツに関する正当な権利を有する者の権利が一層確実に保護されることになる。

【００１４】すなわち、仮に、ファームウェアを介在させずにアプリケーションプログラムから直接に記憶媒体をアクセスすることができるシステムの場合、第１の記憶媒体から第２の記憶媒体に使用権を委譲する前にアプリケーションプログラムで第１の記憶媒体を直接にアクセスして上述した第１の暗号化セキュア情報を読み出して第３の記憶媒体に格納しておく。このような前準備を行なった上で使用権を第１の記憶媒体から第２の記憶媒体に委譲する。その委譲が終了した後、再びアプリケーションプログラムで第１の記憶媒体を直接にアクセスして第３の記憶媒体にあらかじめ復製しておいた委譲前の第１の暗号化セキュア情報を第１の記憶媒体に書き戻す。この場合、第１の記憶媒体は使用権を委譲する前の状態に戻り、かつ第２の記憶媒体にも使用権が発生し、正当な権利者の権利が犯される結果をもたらす。

【００１５】そこで、上記のようにファームウェアのみからアクセスを可能とすることにより、上記のような不正の発生を未然に防止することができ、正当な権利者の権利をより一層確実に保護することができる。

【００１６】

【発明の実施の形態】以下、本発明の実施形態について説明する。ここでは解り易さのため、概念的な実施形態について先ず説明し、次いで具体的な実施形態について説明する。図１は、本発明のライセンス委譲装置の一実施形態を示す構成図、図２は、その説明のための模式図である。

【００１７】図１には、第１の記憶媒体１０、ドライブ２０、および第２の記憶媒体３０が示されている。第１の記憶媒体１０および第２の記憶媒体３０は、いずれも、その記憶媒体の種類を問うものではないが、その記憶媒体を特定するメディアＩＤを有することが必要である。このメディアＩＤは、同種の記憶媒体を互いに確実に識別するものである必要はなく、例えば同一のメディアＩＤを持つ２つの記憶媒体が出会うことがほとんど期待できない程度にその記憶媒体にユニークなものであれ

ばよい。

【００１８】ドライブ２０は、本実施形態では、第１の記憶媒体１０を駆動する第１のドライブ、例えば第１の記憶媒体１０がＭＯ（光磁気ディスク）の場合の光磁気ディスクドライブ装置と、第２の記憶媒体３０を駆動する第２のドライブ、例えば第２の記憶媒体３０がハードディスクの場合そのハードディスクを駆動するハードディスクドライブ装置との複合体として観念される。

【００１９】また、第１のドライブには、そのマイクロコンピュータとそのマイクロコンピュータで動作するソフトウェアとの組合せからなる、第１のドライブにより駆動される第１の記憶媒体をアクセスするための第１のファームウェアが搭載されており、これと同様に、第２のドライブにも、マイクロコンピュータとそのマイクロコンピュータで動作するソフトウェアとの組合せからなる、その第２のドライブにより駆動される第１の記憶媒体をアクセスするための第２のファームウェアが搭載されている。ここでは、第１のファームウェアと第２のファームウェアとの複合体としてのファームウェアがドライブ２０に搭載されているものと観念する。

【００２０】第１の記憶媒体１０および第２の記憶媒体２０は、それぞれ、自分自身のメディアＩＤを記憶しておくＭＩＤエリア１１，３１、使用権情報やその他コンテンツの属性に関する情報が格納されるセキュアエリア１２，３２、およびコンテンツ自身が格納されるユーザエリア１３，３３を有する。ここでは、第１の記憶媒体１０が持っているコンテンツの使用権を第２の記憶媒体３０に委譲しようとしており、したがってここでは、第１の記憶媒体１０のＭＩＤエリア１１，セキュアエリア１２，およびユーザエリア１３には、それぞれ、その第１の記憶媒体１０のメディアＩＤ、使用権情報やその他の属性、およびコンテンツが実際に格納されているものとする。

【００２１】一方、第２の記憶媒体３０のＭＩＤエリア３１には、その第２の記憶媒体３０のメディア３０のメディアＩＤが格納されているが、セキュアエリア３２、およびユーザエリア３３はあらかじめ領域として用意されていてもよく、あるいは、コンテンツの使用権の委譲にあたってそれらの領域が生成されるものであってもよい。

【００２２】以下において説明する復号化手段２１，暗号化手段２２，およびコンテンツ移動手段２３は、ドライブ２０内に搭載されたファームウェア内に構築されており、アプリケーションプログラムは、そのファームウェアを起動することはできるが、そのファームウェアの動作の内部に入り込んでそのファームウェアの動作を制御したり、あるいはそのファームウェアを介在させずに第１の記憶媒体や第２の記憶媒体を直接にアクセスすることはできないように構成されている。

【００２３】つまり、ＭＩＤエリア１１，３１は、ファームウェアによるリードが許可されライトが禁止されているエリアであり、アプリケーションは、ファームウェアを介在させた場合を含めて原則としてＭＩＤエリア１１，３１へのアクセスが禁止されている。また、セキュアエリア１２，３２とユーザエリア１３，３３はファームエリアによるリード・ライトが許可されているエリアであり、アプリケーションは、本実施形態では、ファームエリアを介在させた場合にのみセキュアエリア１２，３２とユーザエリア１３，３３にアクセスすることができ、直接リード・ライトを行うことはできない。但し、ユーザエリア１３，３３については、アプリケーションによる直接的なアクセスが許可されたエリアであってもよい。

【００２４】尚、ＭＩＤエリア１１，３１については、セキュアエリア１２，３２およびユーザエリア１３，３３とは独立に物理的に書き換え不可能な不揮発性の記憶媒体上に設けられていることが望ましい。但し、本実施形態ではＭＩＤエリアはセキュアエリアおよびユーザエリアとともに第１の記憶媒体および第２の記憶媒体上に設けられている。

【００２５】ここで、図２に示すように、第１の記憶媒体１０のユーザエリア１３に格納されたコンテンツは、鍵１で暗号化された形式で格納されており、その鍵１は、使用権情報４１とともに、ＭＩＤエリア１１に格納された、この第１の記憶媒体１０のメディアＩＤからなる鍵２で暗号化された形式で、セキュアエリア１２に格納されている。ここで、図２には、セキュアエリア１２に格納された使用権情報４１として、‘１→０’が示されているが、‘１’はそのコンテンツの使用権が存在することを意味し、‘０’はそのコンテンツの使用権が無いことを意味し、‘１→０’は、使用権の委譲前は‘１’であって、使用権委譲の際に‘０’に書き換えられることを意味している。また、図２において、セキュアエリア１２およびユーザエリア１３は、右にさらに延びるように描かれているが、これは、１つの記憶媒体（ここでは第１の記憶媒体１０）のユーザエリアに複数のコンテンツが格納され、それら複数のコンテンツそれぞれについて鍵や使用権情報等がセキュアエリア１２に格納される場合があることを意味している。

【００２６】ここで鍵１と使用権情報４１を鍵２で暗号化するにあたっては、この図２では、鍵１と使用権情報４１とを合わせた情報が鍵２で暗号化されているように描かれてれているが、そうであってもよく、あるいは、鍵１が鍵２で暗号化され、それとは別に、使用権情報４１が鍵２で暗号化されていてもよい。いずれの場合であっても、鍵２で暗号化された鍵１と、鍵２で暗号化された使用権情報との双方を合わせたものを、ここでは暗号化セキュア情報（本発明にいう第１の暗号化セキュア情報）と称する。

【００２７】コンテンツの使用権の委譲にあたり、図１

に示すドライブ２０の復号化手段２１により、第１の記憶媒体１０のＭＩＤエリア１１に記憶された、第１の記憶媒体１０のメディアＩＤ（本発明にいう第１のメディアＩＤ）からなる鍵２で、セキュアエリア１２に格納された第１の暗号化セキュア情報が復号化され、その暗号化により平文の鍵１と使用権情報４１（ここでは、使用権が存在することを表わす‘１’）が取り出される。そこで、今度は、図１に示すドライブ２０の暗号化手段２２により、その復号化により平文に戻された鍵１と使用権情報４１（使用権が存在することをあらわす‘１’）が今度は、第２の記憶媒体３０のＭＩＤエリア３１に格納されたメディアＩＤ（本発明にいう第２のメディアＩＤ）からなる鍵３で暗号化されて第３の暗号化セキュア情報が生成され、第２の記憶媒体３０のセキュアエリア３２に格納される。図２における第２の記憶媒体３０のセキュアエリア３２に描かれた使用権情報４２が‘０→１’となっているのは、使用権の委譲を受ける前は使用権が存在せず‘０’であって、使用権の委譲を受けることにより使用権が存在することをあらわす‘１’に書き換えられたことを意味する。

【００２８】また、第１の記憶媒体１０には、復号化された使用権情報４１が、使用権が存在しないことをあらわす‘０’に書き換えられ、復号化された鍵１と、使用権が存在しないことをあらわす使用権情報が、第１の記憶媒体１０のメディアＩＤからなる鍵２で暗号化されて、新たな暗号化セキュア情報（本発明にいう第３のセキュア情報）が生成され、それまで第１の記憶媒体１０のセキュアエリア１２に格納されていた第１の暗号化セキュア情報に代えて、その新たに生成された第３のセキュア情報がそのセキュアエリア１２に格納される。

【００２９】あるいは、第１の記憶媒体１０にはそのコンテンツの使用権が存在しなくなったのであるから鍵１は不要であり、第３のセキュア情報を生成して第１の記憶媒体１０のセキュアエリア１２に格納することに代え、そのセキュアエリア１２に暗号化された形式で格納されている鍵１を破壊してしまってもよい。また、第１の記憶媒体１０のユーザエリア１３に格納されている、鍵１で暗号化されたコンテンツは、図１に示すドライブ２０のコンテンツ移動手段２３により、第１の記憶媒体１０から読み出され、鍵１により暗号化された状態のまま、第２の記憶媒体３３のユーザエリア３３に格納される。

【００３０】以上により、それまで第１の記憶媒体１０が所有していた、コンテンツの使用権が、第２の記憶媒体２０に委譲される。それ以降、第２の記憶媒体２０を駆動する第２のドライブでは、アプリケーションプログラムからの、このコンテンツの読出し要求があると、その第２のドライブに搭載された第２のファームウェアは、第２の記憶媒体３０をアクセスし、その第２の記憶媒体３０のＭＩＤエリア３１に格納された、その第２の記憶媒体３０のメディアＩＤからなる鍵３で、セキュアエリア３２に格納された暗号化セキュア情報を復号化し、使用権が存在することを確認し、鍵１により、ユーザエリア３３に格納された、暗号化されたコンテンツを復号化し、その復号化されたコンテンツをアプリケーションプログラムに戻す。

【００３１】一方、その使用権を委譲した後は、第１の記憶媒体１０を駆動する第１のドライブでは、仮に、アプリケーションプログラムからの、その使用権を委譲したコンテンツの読み出し要求があった場合、その第１のドライブに搭載された第１のファームウェアは、第１の記憶媒体１０をアクセスし、その第１の記憶媒体のＭＩＤエリアに格納された、その第１の記憶媒体３０のメディアＩＤからなる鍵２で、そのセキュアエリア１２に格納された暗号化セキュア情報を復号化し、使用権の存在を確認したところ使用権が存在しないことを認識し、あるいは、上述の、鍵１を破壊するシステムの場合は、鍵１が破壊されていること、あるいはそのコンテンツを復号化できないことを認識し、アプリケーションプログラムに対し、そのコンテンツは読み出し不能である旨通知する。このようにして、コンテンツの使用権を、そのコンテンツに関し権利を有する者の権利を犯すことなく、有効に委譲することができる。

【００３２】ここで、上記実施形態では、簡単のため、使用権情報は、使用権が存在することをあらわす‘１’と使用権が存在しないことをあらわす‘０’との二値情報であるとして説明したが、使用可能回数を使用権情報として用いてもよい。例えば委譲前の第１の記憶媒体１０の使用権情報が使用可能回数１０回をあらわす‘１０’であったものとし、その使用可能回数の一部、例えば使用可能回数３回分のみを第２の記憶媒体３０に委譲してもよい。この場合、第２の記憶媒体３０の使用権情報は使用可能回数３回をあらわす‘３’となり、第１の記憶媒体１０には、使用権情報として、使用可能回数７回をあらわす‘７’が書き戻される。第１の記憶媒体１０あるいは第２の記憶媒体３０でそのコンテンツが使用されると、その使用のたびに、第１のドライブに搭載された第１のファームウェアあるいは第２のドライブに搭載された第１のファームウェアにより、その第１の記憶媒体１０あるいは第２の記憶媒体３０の使用可能回数が１ずつ減算される。

【００３３】ここで、第２の記憶媒体３０に委譲した３回分の使用権を使い切ってしまったとき、第１の記憶媒体１０に未だ使用権が残っていればその使用権の一部もしくは全部を上記と同一の手順で再度第２の記憶媒体に委譲することもできる。ただしその場合は、暗号化されたコンテンツ自体は既に第２の記憶媒体３０に移っているため、そのコンテンツ自体を第２の記憶媒体３０に移す必要はなく、そのコンテンツの使用権のみを第２の記憶媒体３０に移せばよい。

【００３４】尚、図２に示す例では、鍵１と使用権情報との双方を１つの情報と見なして、その情報を鍵２で暗号化することにより第１の記憶媒体１０用の暗号化セキュア情報を生成し、鍵１と使用権情報との双方を１つの情報とみなしてその情報を鍵３で暗号化することにより第２の記憶媒体３０用の暗号化セキュア情報を生成しているが、鍵１と使用権情報は、別々に暗号化してもよい。その場合、使用権の委譲にあたって鍵１は既に暗号化された形式で第１の記憶媒体１０に格納されているため、新たな使用権情報のみを暗号化して第１の記憶媒体１０に書き戻せばよい。また、使用可能回数を複数回に分けて委譲する場合、２回目以降の委譲の際は、第２の記憶媒体３０には鍵１が鍵３で暗号化された形式で既に格納されているため、委譲を受けた使用可能回数をあらわす使用権情報のみを鍵３で暗号化してセキュアエリア３２に書き込めばよい。

【００３５】また、鍵１と使用権情報のほか、例えばそのコンテンツの名称、そのコンテンツの最終アクセス日時等そのコンテンツの使用権情報以外の属性も一緒にセキュアエリアに格納してもよく、その場合に、それらの属性が暗号化する必要がないものである場合は平文のまま格納してもよく、あるいはそれらの属性が暗号化する必要がないものであっても、鍵１や使用権情報と一緒に暗号化してもよい。

【００３６】さらに、上記では使用権情報として、使用権の有無と、使用回数を取り挙げて説明したが、そのほかにも、使用可能時間を使用権情報としてもよく、アクセスが許諾された人をあらわすＩＤを使用権情報としてもよく、使用権の有無、あるいは使用可能範囲をあらわす種々の情報を使用権情報として使用することができる。

【００３７】図３は、本発明のライセンス委譲装置の一実施形態が搭載されたコンピュータシステムの一例を示す外観斜視図、図４は、そのコンピュータシステムの構成を示すブロック図である。このコンピュータシステム５０は、外観上は、図３に示すように、ＣＰＵやメモリ等が内蔵された本体部５１、表示画面５２ａ上に画像を表示する画像表示装置５２、このコンピュータシステム５０に対し各種の指示を行なうための操作子であるキーボード５３、および画像表示装置５２の表示画面５２ａ上の位置を指定するための操作子であるマウス５４により構成されている。また本体部５１には、ＭＯ（光磁気ディスク）１００が装填、取出し自在に装填されるＭＯ装填口５１ａが示されている。

【００３８】また、このコンピュータシステム５０は、内部構成上は、図４に示すように、各種のプログラムが実行されるＣＰＵ５５、実行されるプログラムやデータの一時的な格納領域として使用されるメモリ５６、キーボード５３との間でデータの受け渡しを行なうキーボードインターフェース５７、マウス５４の操作に伴うデータを伝えるマウスインターフェース５８、画像表示装置５２に表示用のデータを伝える表示インターフェース５９、図３に示すＭＯ装填口５１から装填されたＭＯ１００を駆動するＭＯドライブ６０、および内蔵されたハードディスク６２を駆動するハードディスクドライブ６１が備えられており、それらは、図４に示すように、バス６３で互いに接続されている。

【００３９】ここでは、図３，図４に示すコンピュータシステム５０内において、ＭＯ１００に格納されたコンテンツの使用権をハードディスク６２に委譲する場合を説明するが、使用権の単純な移動、あるいは、使用可能回数が設定されている場合において、その使用可能回数以内の一部の使用可能回数を初回に委譲する場合については、図１，図２を参照して既に説明済であるため、以下では、初回に委譲した使用可能回数を使い果たし、所定の使用可能回数を再度委譲する場合について説明する。また、図１，図２を参照した説明は、本発明の理解のために概念的な説明を行なったが、ここではより詳細な説明を行なう。

【００４０】図５は、ＭＯ１００に格納されたコンテンツの使用権をハードディスク６２に委譲する手順を示す図である。この図５には、アプリケーション６４とドライブ２０が示されている。アプリケーション６４は、ＣＰＵ５５で実行される、コンピュータシステム５０の操作者により直接に操作が可能なプログラムであって、ここでは、ＭＯ１００内のコンテンツの使用権をハードディスク６２に委譲することを指示するプログラムをあらわしている。また、ドライブ２０は、ここでは、図４に示すＭＯドライブ６０とハードディスクドライブ６１との複合体である。ＭＯ１００に格納されたコンテンツの使用権をハードディスク６２に委譲する手順を以下に説明するが、ここではＭＯ１００に、委譲しようとしているコンテンツを残り１０回使用することができる使用権が残っており、そのうちの３回の使用権をハードディスク６２に委譲するものとして説明する。

【００４１】ここでは簡単のため、委譲され得るコンテンツは１つのみ存在するものとし、コンテンツと称するときは、その委譲される（あるいはその委譲によりハードウェア６２に使用権が移った）コンテンツを意味するものとする。

（１）先ず、アプリケーション６４からドライブ２０に向けて、コンテンツの委譲元がＭＯ１００であり、コンテンツの委譲先がハードディスク６２であることを、ドライブ２０に向けて指定する（図５（Ａ））。

【００４２】（２）するとドライブ２０は、ＭＯ１００およびハードディスク６２をアクセスするための準備を行ない、ドライブ２０は、それらの準備が整った段階で、アプリケーション６４に対し準備が整ったことを報告する（図５（Ｂ））。

（３）すると、アプリケーション６４では、ドライブ２

０がアプリケーションに送る情報を隠蔽するためのパスワードをドライブ２０（ＭＯドライブ６０とハードディスクドライブ６１との双方）に送るとともに、ＭＯ１００のセキュアエリア（図１，図２参照）に格納されている使用権情報（ここでは、上述の前提どおり、使用可能回数をあらわす情報を使用権情報としており、ＭＯ１００には、現在１０回使用可能であることをあらわす使用権情報‘１０’が格納されているものとする）を読み出す命令をドライブ２０に向けて発行する（図５（Ｃ））。

【００４３】（４）すると、ドライブ２０を構成するＭＯドライブ６０（図４参照）内では、以下の処理が実行される。ここで、ＭＯドライブ６０内にもＣＰＵが搭載されており、さらに、装填されたＭＯ１００をアクセスするためのマイクロプログラムが搭載されており、それらＭＯドライブ６０のハードウェアとソフトウェアとを合せたファームウェアがＭＯドライブ６０における処理を実行することになる。

【００４４】（４－１）ＭＯ１００のＭＩＤエリア（図１，図２のＭＩＤエリア１１参照）からＭＯ１００のメディアＩＤを読み出す。

（４－２）ＭＯ１００のセキュアエリア（図１，図２のセキュアエリア１２参照）から、メディアＩＤで暗号化された使用権情報を読み出す。

（４－３）その読み出した使用権情報をメディアＩＤで復号化する。

【００４５】（４－４）上述（３）のステップにおいてアプリケーション６４から送られてきたパスワードで、復号化された使用権情報をエンコードする。

（４－５）そのエンコードされた情報をアプリケーション６４に伝える（図５（Ｄ））。

（５）すると、アプリケーション６４は、以下の処理を実行する。

【００４６】（５－１）ＭＯドライブ６０から送られてきた使用権情報をパスワードでデコードする。

（５－２）そのデコードされた使用権情報があらわす使用可能回数がこれ以上使用できないことをあらわす‘０’でないことを確認する（ここでは、説明の前提として使用可能回数１０回をあらわす‘１０’が設定されており、‘０’ではない）。

【００４７】（５－３）今度は、ドライブ２０に向けて、使用権の委譲先であるハードディスク６２の、使用権情報を読み出す命令を発行する（図５（Ｅ））。尚、前述したように、ここでは説明の前提として、ハードディスク６２には、前回、コンテンツを何回か使用することのできる使用権が設定され、その使用可能回数が‘０’になった場合を想定している。

【００４８】（６）すると、ハードディスク６２を駆動するハードディスクドライブ６１では以下の処理が実行される。ハードディスクドライブ６１にもＣＰＵやマイクロプログラムが備えられており、ハードディスクドライブ６１における処理も、ＭＯドライブ６０における処理と同様、それらハードウェアとソフトウェアとの複合体としてのファームウェアにより実行される。

【００４９】（６－１）ハードディスク６２のＭＩＤエリア（図１，図２のＭＩＤエリア３１参照）からハードディスク６２のメディアＩＤを読み出す。

（６－２）ハードディスク６２のセキュアエリア（図１，図２のセキュアエリア３２参照）から、ハードディスク６２のメディアＩＤで暗号化された使用権情報を読み出す。

【００５０】（６－３）その読み出した使用権情報を、ハードディスク６２のメディアＩＤで復号化する。

（６－４）上述の（３）のステップにおいてアプリケーション６４から送られてきたパスワードで、その復号化された使用権情報をエンコードする。（６－５）そのエンコードされた使用権情報をアプリケーション６４に伝える（図５（Ｆ））。

【００５１】（７）すると、アプリケーション６４は、以下の処理を実行する。

（７－１）ハードディスクドライブ６１から送られてきた使用権情報をパスワードでデコードする。

（７－２）そのデコードされた使用権情報が使用可能回数‘０’をあらわしていることを確認する。

【００５２】もし使用可能回数が‘０’でなく、まだ使用可能であることをあらわしているときは、本実施形態では、まだ使用可能である旨表示画面５２ａ（図３参照）に表示してオペレータにその旨通知し、この段階で処理を中断する。ここでは説明の前提として使用可能回数は‘０’であり、この場合、さらに以下の処理に進む。

【００５３】（７－３）ハードディスク６２に新たに設定される使用可能回数（ここでは説明の前提に基づいて３回）をあらわす情報（新回数情報と称する）をパスワードでエンコードしてドライブ２０（ＭＯドライブ６０とハードディスクドライブ６１との双方）に送る（図５（Ｇ））。

（８）ＭＯドライブ６０では、この新回数情報を受けて以下の処理が実行される。

【００５４】（８－１）ＭＯ１００のメディアＩＤを読み出す。

（８－２）ＭＯ１００のセキュアエリアに格納されている、ＭＯ１００のメディアＩＤで暗号化された状態の使用権情報を読み出す。

（８－３）その暗号化された使用権情報をＭＯ１００のメディアＩＤで復号化して使用可能回数‘１０’を取り出す。

【００５５】（８－４）アプリケーション６４から送られてきた、パスワードでエンコードされた新回数情報を、上述の（３）のステップで送られてきているパスワ

ードでデコードして使用可能回数‘３’を取り出す。
（８－５）ＭＯ１００にそれまで格納されていた使用可能回数‘１０’からハードディスク６２に譲渡しようとしている使用可能回数‘３’を差し引いて新たな使用可能回数‘７’を得る。
（８－６）その新たな使用可能回数‘７’をあらわす新たな使用権情報をＭＯ１００のメディアＩＤで暗号化する。
【００５６】（８－７）その暗号化された新たな使用権情報を、それまでＭＯ１００に格納されていた、使用可能回数‘１０’をあらわす使用権情報に上書きする。これにより、ＭＯ１００には使用可能回数‘７’が設定される。
（９）一方、ハードディスクドライブ６１では、上述の（７－３）のステップで送られてきた新回数情報を受けて、以下の処理が実行される。
【００５７】（９－１）ハードディスク６２のメディアＩＤを読み出す。
（９－２）アプリケーション６４から送られてきた、パスワードでエンコードされた新回数情報を、上述の（３）のステップで送られてきているパスワードでデコードして使用可能回数‘３’を取り出す。
（９－３）そのデコードにより取り出された使用可能回数‘３’をあらわす新たな使用権情報をハードディスク６２のメディアＩＤで暗号化する。
【００５８】（９－４）その暗号化された新たな使用権情報を、ハードディスク６２に格納されていた、使用可能回数‘０’をあらわす使用権情報に上書きする。これにより、ハードディスク６２には、使用可能回数‘３’が設定される。
（１０）以上の使用権委譲の処理が完了したことが、ドライブ２０からアプリケーション６４に通知される。
【００５９】以上のようにしてコンテンツの使用権の委譲（ここでは使用権の一部の委譲）が行なわれる。尚、図５を参照した以上の説明では、ＭＯ１００からハードディスク６２への、コンテンツ自体および暗号化されたコンテンツを復号化するための鍵の移動については言及されていないが、前述したように、ここでは、コンテンツの使用可能回数の再度の設定の場合を説明しており、したがってコンテンツ自体および、それを復号化するための鍵は初回の委譲時に既にハードディスク６２に渡されていることを前提としている。コンテンツ自体は、ＭＯ１００から初回の委譲時に暗号化された形式のままハードディスク６２に移動（複製）されており、また上記の説明は、鍵はそれぞれのメディアＩＤで使用権情報とは独立に暗号化されてそれぞれのセキュアエリアに格納されていることを前提としている。
【００６０】尚、図５を参照して説明した実施形態では、上述したように、アプリケーション６４とドライブ２０とが様々なコミュニケーションを行ないながらコンテンツの使用権の委譲の処理を進めているが、このようなコンテンツ委譲処理に代え、アプリケーション６４からは、使用権を委譲しようとしているコンテンツ、そのコンテンツの使用権の委譲元（ここではＭＯ１００）、委譲先（ここではハードディスク６２）、および委譲しようとしている、使用権の回数を指定し、その後はドライブ２０（ここではＭＯドライブ６０とハードディスクドライブ６１との双方）に処理を任せ、アプリケーション６４とは独立にドライブ２０において上記の委譲処理を実行し、委譲処理が終了した段階、および何らかの不都合により委譲処理が正常に行なわれなかった（例えばＭＯ１００に委譲を指定された使用可能回数未満の使用可能回数しか残っていなかった、あるいはハードディスク６２に前回に委譲を受けた使用可能回数がまだ‘０’になっていなかった、など）ときのみ、アプリケーション６４に報告するように構成してもよい。
【００６１】また、上記の委譲処理６０は、上記の説明ではＭＯドライブ６０とハードディスクドライブ６１とで分担して実行しているが、それらＭＯドライブとハードディスクドライブ６１とのうちの一方はアクセス専用とし、上記の委譲処理は、専らもう一方の側で行なうように構成してもよい。図６は、本発明のライセンス委譲装置の一実施形態が組み込まれたコンピュータネットワークの一例を示す図、図７は、そのコンピュータネットワークを構成するあるコンピュータシステムから別のコンピュータシステムに対し、コンテンツの使用権を委譲する際の手順を示す図である。
【００６２】ここには、コンテンツ管理用のコンピュータシステム７０と、コンテンツを使用する側の２台のコンピュータシステム８０，９０が示されており、それら３台のコンピュータシステム７０，８０，９０は、通信回線２００を介して互いに接続されている。各コンピュータシステム７０，８０，９０は、それぞれが図３に示すコンピュータシステム５０と同様の構成を備えている。すなわち、各コンピュータシステム７０，８０，９０は、各本体部７１，８１，９１、各画像表示装置７２，８２，９２、各キーボード７３，８３，９３および各マウス７４，８４，９４を備えており、さらに各コンピュータシステム７０，８０，９０は、それぞれが図４に示す内部構成と同様の内部構成を備えている。詳細説明は省略する。
【００６３】ここでは、コンテンツ管理用のコンピュータシステム７０は、ある会社の本店に設置され、コンテンツを使用する側のコンピュータシステム８０，９０はその会社の各支店に設置されているものとする。以下では、説明の簡単のため、本店、および各支店に設置されたコンピュータシステム７０，８０，９０を、そのまま本店７０、支店８０、支店９０と称する。
【００６４】ここでは本店で、各種のコンテンツの全支店分のライセンスを購入し、その本店から各支店にライ

センスを分配し、かつ、その本店で全支店分のライセンスを管理しているものとする。すなわち、ここでは、同一のコンテンツであっても本店において必要な数の使用権を購入し、そのコンテンツを必要とする支店にその使用権を分配する。ここでいう同一のコンテンツについての必要な数の使用権は、そのコンテンツの使用回数を意味するものではなく、同一の本を複数冊（例えば３冊）購入するのと同様に同一のコンテンツの使用権を必要に応じた数だけ購入し、ここではその購入した数の使用権を意味している。本店では、各コンテンツについて、購入した使用権の数から支店に対し使用権を頒布した数の残りの数が管理されており、各支店では、同一のコンテンツについての複数の使用権は不要であって、各コンテンツについて自分の支店に使用権が存在するか否かのみを管理している。本店および各支店では多数のコンテンツの使用権情報が管理されており、ここではそれら多数のコンテンツの使用権情報の一覧を‘許諾情報’と称する。

【００６５】ここでは、本店７０から各支店８０，９０に対し、既に様々なコンテンツの使用権が委譲されており、さらに今回、本店７０からある支店（ここでは支店８０とする）に対しあるコンテンツの使用権を委譲するものとし（ここでは、使用権の新たな委譲を行なおうとしているコンテンツを‘新コンテンツ’と称する）、ここでは、その新コンテンツの使用権を支店８０に委譲する場面について説明する。ここでは、新コンテンツの使用権は、本店７０のハードディスクから支店８０のハードディスクに委譲されるものとする。

【００６６】（１）先ず本店７０から支店８０に向けて新コンテンツの使用権を委譲する旨連絡する（図７（Ａ））。

（２）すると支店８０ではその連絡を受けて、支店８０のハードディスクを準備状態にし、アクセスの準備が整うと本店７０に対し準備ができたことを報告する（図７（Ｂ））。

【００６７】（３）すると本店７０では、支店８０から送られてくる情報を隠蔽するためのパスワードを支店８０に送出し、さらに支店８０のハードディスクのセキュアエリアに格納されている許諾情報（複数のコンテンツそれぞれの使用権の有無をあらわす情報の一覧）を送るよう命令を発行する（図７（Ｃ））。

（４）支店８０では、この命令を受けて以下の処理を実行する。

【００６８】（４－１）支店８０のハードディスクのメディアＩＤを読み出す。

（４－２）支店８０のハードディスクのセキュアエリアから、そのハードディスクのメディアＩＤで暗号化された許諾情報を読み出す。

（４－３）その読み出した許諾情報を読み出したメディアＩＤで復号化する。

（４－４）上記の（３）のステップにおいて本店７０から送られてきたパスワードで、その復号化された許諾情報と、さらに支店８０のハードディスクのメディアＩＤをエンコードする。

【００６９】（４－５）そのエンコードされた許諾情報およびメディアＩＤを本店７０に送る（図７（Ｄ））。

（５）すると、本店７０では、以下の処理を実行する。

（５－１）支店８０から送られてきた許諾情報およびメディアＩＤをパスワードでデコードする。

【００７０】（５－２）そのデコードされた許諾情報を見て、これから支店８０に使用権を移そうとしている新コンテンツに関する使用権が支店８０に存在しないことを確認する。これは、同一の支店に対し同一のコンテンツの使用権を重複設定するのを避けるためである。

（５－３）本店７０のハードディスクのメディアＩＤを読み出す。

【００７１】（５－４）本店７０のハードディスクのセキュアエリアから、そのハードディスクのメディアＩＤで暗号化された許諾情報、および、同じくそのメディアＩＤで暗号化された、使用権を許諾しようとしているコンテンツを復号化するための鍵を読み出す。

（５－５）その読み出した許諾情報および鍵を、読み出したメディアＩＤで復号化する。

【００７２】（５－６）その復号化された許諾情報を参照して、支店８０に使用権をあらたに委譲しようとしているコンテンツ（新コンテンツ）に関する使用権に残りがあることを確認する。残りがないときは、その新コンテンツの使用を許諾することができない旨支店８０に伝えることになるが、ここでは、その新コンテンツの使用権が本店７０に残っているものとする。

【００７３】（５－７）上記の（５－１）のステップでデコードした、支店８０の許諾情報中の、新コンテンツの使用権をあらわす情報を‘使用権なし’から‘使用権有り’に書き換える。

（５－８）その書き換えた許諾情報、および鍵の双方をパスワードでエンコードする。

【００７４】（５－９）本店７０のハードディスクのユーザエリアから、暗号化された新コンテンツを読み出す。

（５－１０）そのエンコードされた許諾情報および鍵、および暗号化されたままの新コンテンツを支店８０に送る（図７（Ｅ））。

（５－１１）また、本店７０内において、上記の（５－５）のステップで復号化した本店７０の許諾情報中の、支店８０に今回使用権を許諾した新コンテンツに関する使用権の数に関する情報を１だけ減算することにより新たな許諾情報に更新する。

【００７５】（５－１２）そのようにして更新された新たな許諾情報を、本店７０のハードディスクのメディアＩＤで暗号化する。

（５－１３）その暗号化された新たな許諾情報を、本店７０のハードディスクのセキュアエリアに、そこにそれまで格納されていた更新前の許諾情報に代えて格納する。

【００７６】（６）支店８０では、上記の（５－１０）のステップで送られてきた、エンコードされた許諾情報および鍵、および暗号化された新コンテンツを受け取り、以下の処理を実行する。

（６－１）受け取った新コンテンツを、暗号化されたまま自分（支店８０）のハードディスクのユーザエリアに格納する。

【００７７】（６－２）受け取った許諾情報および鍵を、上述のステップ（３）で送られてきているパスワードでデコードする。

（６－３）自分（支店８０）のハードディスクのメディアＩＤを読み出す。

（６－４）パスワードでデコードされた許諾情報および鍵を、その読み出したメディアＩＤで暗号化する。

【００７８】（６－５）その暗号化された許諾情報および鍵を、自分（支店８０）のハードディスクのセキュアエリアに、それまで格納されていた許諾情報を書き換えるようにして格納する。以上により、その新コンテンツの使用権が本店７０から支店８０に委譲される。

【００７９】以上の各実施形態に示すように、本発明のライセンス委譲装置は、１台のコンピュータ等からなる１台の装置内においても、あるいは複数台のコンピュータ等を接続したネットワーク内においても実現可能である。

【００８０】

【発明の効果】以上説明したように、本発明によれば、コンテンツに関し権利を有する者の権利を犯すことなく、そのコンテンツを複製したり頒布したりすることができる。

【図面の簡単な説明】

【図１】本発明のライセンス委譲装置の一実施形態を示す構成図である。

【図２】図１に示すライセンス委譲装置の説明のための模式図である。

【図３】本発明のライセンス委譲装置の一実施形態が搭載されたコンピュータシステムの一例を示す外観斜視図である。

【図４】図３に外観を示すコンピュータシステムの構成を示すブロック図である。

【図５】ＭＯに格納されたコンテンツの使用権をハードディスクに委譲する手順を示す図である。

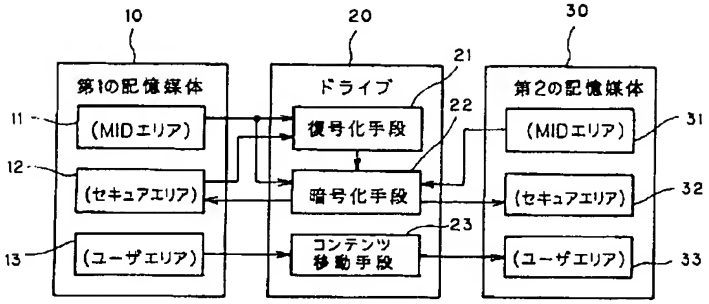
【図６】本発明のライセンス委譲装置の一実施形態が組み込まれたコンピュータネットワークの一例を示す図である。

【図７】図６に示すコンピュータネットワークを構成するコンピュータシステムから別のコンピュータシステムに対し、コンテンツの使用権を委譲する際の手順を示す図である。

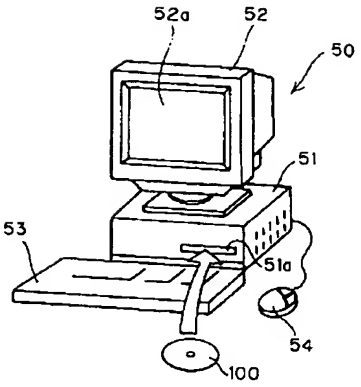
【符号の説明】

１０　第１の記憶媒体
１１　ＭＩＤエリア
１２　セキュアエリア
１３　ユーザエリア
２０　ドライブ
２１　復号化手段
２２　暗号化手段
２３　コンテンツ移動手段
３０　第２の記憶媒体
３１　ＭＩＤエリア
３２　セキュアエリア
３３　ユーザエリア
４１，４２　使用権情報
５０　コンピュータシステム
５１　本体部
５１ａ　ＭＯ装填口
５２　画像表示装置
５２ａ　表示画面
５３　キーボード
５４　マウス
５５　ＣＰＵ
５６　メモリ
５７　キーボードインターフェース
５８　マウスインターフェース
５９　表示インターフェース
６０　ＭＯドライブ
６１　ハードディスクドライブ
６２　ハードディスク
７０，８０，９０　コンピュータシステム
７１，８１，９１　本体部
７２，８２，９２　画像表示装置
７３，８３，９３　キーボード
７４，８４，９４　マウス
１００　ＭＯ（光磁気ディスック）
２００　通信回線

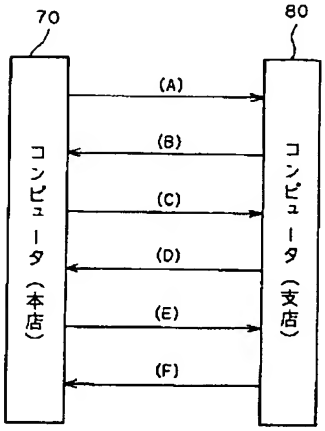
【図１】


10
20
30
第1の記憶媒体
ドライブ
第2の記憶媒体
11
(MIDエリア)
12
(セキュアエリア)
13
(ユーザエリア)
21
復号化手段
22
暗号化手段
23
コンテンツ移動手段
(MIDエリア)
31
(セキュアエリア)
32
(ユーザエリア)
33

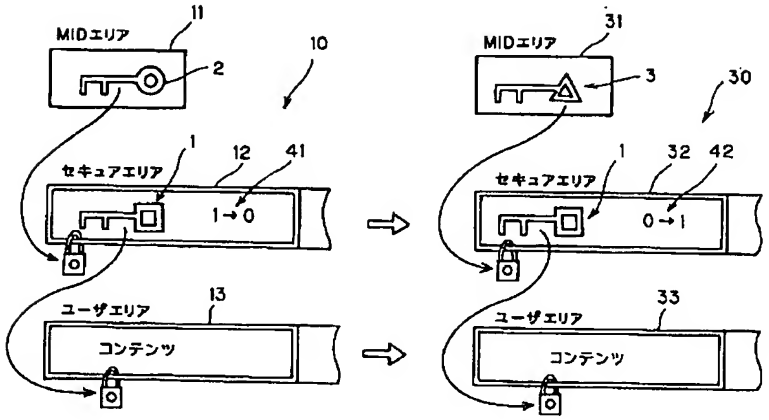
【図３】


52a
52
50
51
53
51a
54
100

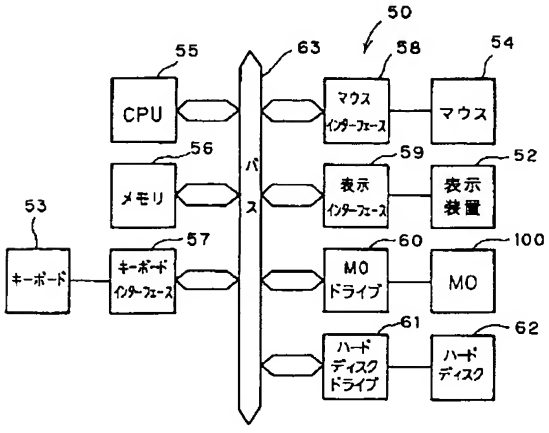
【図７】


70
80
コンピュータ（本店）
コンピュータ（支店）
(A)
(B)
(C)
(D)
(E)
(F)

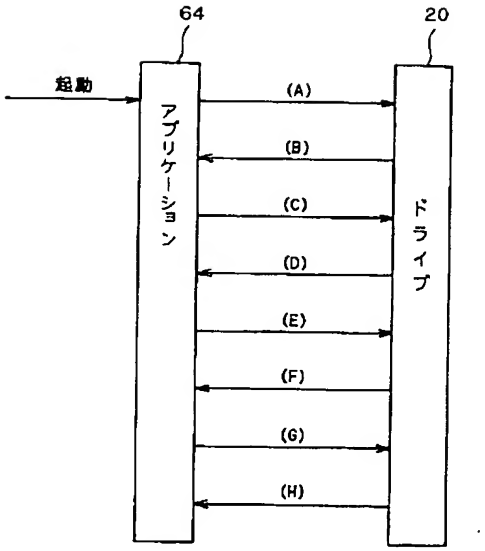
【図２】


MIDエリア
11
2
10
セキュアエリア
1
12
41
1→0
ユーザエリア
13
コンテンツ
MIDエリア
31
3
30
セキュアエリア
1
32
42
0→1
ユーザエリア
33
コンテンツ

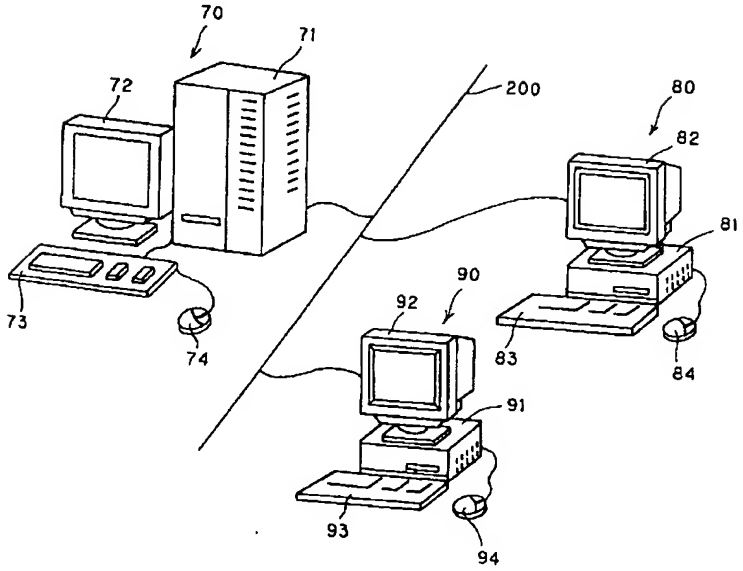
【図４】


50
55
63
58
54
CPU
マウスインターフェース
マウス
56
59
52
メモリ
表示インターフェース
表示装置
53
57
60
100
キーボード
キーボードインターフェース
MOドライブ
MO
61
62
ハードディスクドライブ
ハードディスク
バス

【図５】


64
20
起動
アプリケーション
ドライブ
(A)
(B)
(C)
(D)
(E)
(F)
(G)
(H)

【図６】


70
71
72
200
80
82
81
90
92
91
73
74
83
84
93
94

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-328033

(43)Date of publication of application : 30.11.1999

---

(51)Int.Cl. G06F 12/14
G06F 17/60
G09C 1/00

---

(21)Application number : 10-138663 (71)Applicant : FUJITSU LTD

(22)Date of filing : 20.05.1998 (72)Inventor : UCHIUMI KENICHI
HIRANO HIDEYUKI
KOTANI MASATAKE

---

(54) LICENSE TRANSFER DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To copy and deliver contents while protecting a person having a right to the use of the contents in a license transfer system which transfers the right to the use of contents.

SOLUTION: Contents are enciphered with a key 1, and this key 1 and information on use right 41 are enciphered with a key 2 consisting of a medium ID which specifies a storage medium 10 where they are stored. At the time of transferring the right to the use of the contents, contents enciphered by the key 1 are transferred to a storage medium 30 of a transfer destination as they are, and the key 1 and use right information 41 are deciphered by the medium ID of the storage medium of the transfer

source and are enciphered by the medium ID of the storage medium of the transfer destination and are stored in the storage medium 30 of the transfer destination.

CLAIMS

[Claim(s)]

[Claim 1]Contents enciphered with a predetermined key characterized by comprising the following, The 1st storage with which the 1st encryption secure information that it came to encipher both sides of 1st media ID that specifies itself, and the 1st royalty information showing a royalty of said key and these contents by said 1st media ID together or independently was stored, A license transfer device which transfers a royalty of contents which accessed the 2nd storage with which 2nd media ID that specifies itself was stored, and were stored in said 1st storage to said 2nd storage from said 1st storage.

A key obtained by decryption by decoding means which acquires said key and said 1st royalty information by decrypting the 1st encryption secure information stored in said 1st storage in a transfer of a royalty of said contents using said 1st media ID, and said decoding means.

By decryption by said decoding means. When the 1st royalty that the 1st obtained royalty information expresses enciphers that it is together or independently both sides with the 2nd royalty information showing the 2nd royalty transferred or apportioned by said 2nd media ID. An encoding means which generates the 2nd encryption secure information and is made to store in

said 2nd storage.

[Claim 2]Said encoding means the 3rd royalty information that expresses the 3rd royalty after deducting said 2nd royalty from said 1st royalty further, or said key -- this -- by enciphering by said 1st media ID and returning both sides with the 3rd royalty information to said 1st storage, replacing with this 1st storage at said 1st encryption secure information -- both sides of said key and said 3rd royalty information -- this -- the license transfer device according to claim 1 being a thing in which the 3rd encryption media information which it comes to encipher by 1st media ID is made to store.

[Claim 3]A key from which said encoding means was acquired by decryption by said decoding means when the whole royalty of said contents which said 1st storage has was transferred to said 2nd storage, While generating the 2nd encryption secure information that it comes to encipher the 2nd royalty information showing the 2nd royalty that inherited said all 1st royalty and making it store in said 2nd storage, The license transfer device according to claim 1 being a thing which makes said key which constitutes said 1st encryption secure information stored in said 1st storage destroy.

[Claim 4]. Said 1st storage was enciphered before a royalty transfer of contents. Contents as which a candidate for a transfer which contents which are going to transfer a royalty were stored and was stored in said 1st storage in a transfer of a royalty of contents was enciphered are read, The license transfer device according to claim 1 having a contents transportation device stored in said 2nd storage with the state where it was enciphered.

[Claim 5]The license transfer device according to claim 1 which said 1st royalty information and said 2nd royalty information mean that a royalty exists, and is characterized by said 3rd royalty information being a thing showing a royalty not existing.

[Claim 6]Said 1st royalty information is a thing showing the 1st number of times of usable or available time, said 2nd royalty information -- this -- the 2nd number of times of usable or available time within the 1st number of times of usable or available time being expressed, and, said 3rd royalty information -- this -- from the 1st number of times of usable or available time -- this -- the license transfer device according to claim 1 being a thing showing the 3rd number of times of usable or available time after deducting the 2nd number of times of usable or available time.

[Claim 7]While having the 1st drive and drive of the 2nd that drive said 1st storage and said 2nd storage, respectively, . This 1st drive and this 2nd drive access said 1st storage and said each of 2nd storage. It has the 1st firmware and 2nd firmware, respectively, Said decoding means and said encoding means are constituted in firmware as a complex of said 1st firmware and said 2nd firmware, While only said 1st firmware has the title which accesses said 1st storage driven by said 1st drive, The license transfer device according to claim 1 being what has the title to which only said 2nd firmware accesses the 2nd storage driven by said 2nd drive.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the license transfer device which transfers the royalty of contents to the 2nd storage from the 1st storage.

[0002]

[Description of the Prior Art]In recent years, how efficiency of protection of copyright is attained is posing a problem. For example, although distributing itself is not accompanied by a duplicate in the case of material being like a book,

as for the book, a book will not exist in a vender's basis over a buyer's hand if a book is resold, therefore protection of copyright is comparatively easy, In the case of the digital-information-ized works, if the digitized works are transmitted via a network, for example, it will be generated the oneself side by the same works as both sides with the other party, A result on which distributing itself follows a duplicate is brought, and effectual protection of the copyright over such digital-information-ized works is usually made very difficult.

[0003]

[Problem(s) to be Solved by the Invention]An object of this invention is to provide a license transfer device transferable [aiming at protection of those who have a right for the royalty of contents, such as a document, a movie a program, etc. which were digitized about the contents in view of the above-mentioned situation].

[0004]

[Means for Solving the Problem]A license transfer device of this invention which attains the above-mentioned purpose, Contents enciphered with a predetermined key, and 1st media ID that specifies itself, The 1st storage with which the 1st encryption secure information that it came to encipher both sides

with the 1st usage information showing a royalty of the above-mentioned key and its contents by 1st media ID together or independently was stored, In a license transfer device which transfers a royalty of contents which accessed the 2nd storage with which 2nd media ID that specifies itself was stored, and were stored in the 1st storage to the 2nd storage from the 1st storage, A key obtained by decryption by decoding means which acquires the above-mentioned key and royalty information on the above 1st by decrypting the 1st encryption secure information stored in the 1st storage in a transfer of a royalty of contents using 1st media ID, and the above-mentioned decoding means, By and decryption by the above-mentioned decoding means. When the 1st royalty that the 1st obtained royalty information expresses enciphers that it is together or independently both sides with the 2nd royalty information showing the 2nd royalty transferred or apportioned by media ID of the above 2nd. It had an encoding means which generates the 2nd encryption secure information and is made to store in the 2nd storage.

[0005]In a license transfer device of above-mentioned this invention here the above-mentioned encoding means, The 3rd royalty information showing the 3rd royalty after deducting the 2nd royalty of the above from the 1st royalty of the

above, Or by enciphering by media ID of the above 1st and returning both sides of a key and royalty information on the abóve 3rd to the 1st storage, It may be a thing in which replace with the 1st storage at encryption secure information on the account 1st of the above, and both sides of the above-mentioned key and royalty information on the above 3rd make the 3rd encryption media information which it comes to encipher by 1st media ID store, Or when transferring the whole royalty of the above-mentioned contents which the 1st storage has to the 2nd storage, the above-mentioned encoding means, While generating the 2nd encryption secure information that it comes to encipher a key obtained by decryption by the above-mentioned decoding means, and the 2nd royalty information showing the 2nd royalty that inherited all the 1st royalty of the above and making it store in the 2nd storage, A key which constitutes the 1st encryption secure information stored in the 1st storage may be made to destroy.

[0006]above-mentioned "key and .... the -- both sides with royalty information on one 1st encryption secure information" which it comes to encipher by 1st media ID that it is together or independently, Encipher a key by 1st media ID and the 1st royalty information is enciphered by the 1st media information apart from this, What doubled the 1st royalty information enciphered as those enciphered keys

may be called the 1st encryption secure information, Or what put both sides of a key and the 1st royalty information in a row is enciphered by the 1st media information, and it means that the enciphered information may be called the 1st encryption secure information.

[0007]above-mentioned "key and .... the -- both sides of royalty information on two -- together -- or -- separate .... the -- Generate the 2nd encryption secure information by enciphering by media ID of two.... with " and "key. .... the 3rd encryption secure information which it comes to encipher by 1st media ID" has same both sides with royalty information which is the 3. the above -- "-- the 3rd royalty information -- or .... a key .... the -- both sides with royalty information on three .... the -- Encipher by media ID of one.... ", In a system which enciphers independently the 1st royalty information or the 2nd royalty information as a key, In a system which should encipher only the 3rd royalty information and enciphers what put a key and the 1st (or the 2nd) royalty information in a row, it means enciphering what put both sides of a key and the 3rd royalty information in a row.

[0008]A license transfer device of this invention is completed paying attention to a point that ID (media ID is called) peculiar to each is given, for example to MO

(magneto-optical disc) or a hard disk. It is unusable unless the enciphered contents themselves are decrypted using the key by circulating contents enciphered with a predetermined key. Then, a key for decrypting the enciphered contents and both sides with royalty information, including for example, information whether use of the contents is permitted etc., are enciphered by media ID original with the storage. By carrying out like this, the enciphered contents, Unapproved use by those who use is impossible, cannot decrypt a key since media ID differs at the point which received distribution if a key was also distributed as it was even if the contents leave a storage stored from the first and itself is distributed, therefore do not have a royalty can be prevented.

[0009]In such a system, in order to convey one's (the 1st storage) royalty to a transfer place (the 2nd storage), In the range of one's royalty (for example, usable number of times of survival), decrypt a key and one's royalty information by one's (the 1st storage) media ID, apportion a royalty (or it may be the whole royalty), and A key, the -- or it was apportioned, it enciphers by media ID (2nd media ID) of a transfer place (the 2nd storage), and royalty information as the whole is made to store in the transfer place (the 2nd storage) For themselves (the 1st storage), the remaining royalties (a royalty that a royalty does not exist is

included) are enciphered by their (the 1st storage) media ID (1st media ID), and it returns itself (the 1st storage). Or when transferring all of royalties, in itself (the 1st storage), a key stored in form enciphered by it (the 1st storage) may be destroyed instead of enciphering the remaining royalties (in this case, royalty that a royalty does not exist), and returning. Transfer of a royalty is attained by carrying out like this, without infringing on a right of those who have a right about the contents.

[0010]Here a license transfer device of above-mentioned this invention, . The 1st storage was enciphered before a royalty transfer of contents. Contents as which a candidate for a transfer which contents which are going to transfer a royalty were stored and was stored in the 1st storage in a transfer of a royalty of contents was enciphered are read, It is preferred to have a contents transportation device stored in the 2nd storage with the state where it was enciphered.

[0011]Since the contents themselves are distributed with the state where it was enciphered, it may distribute any time, For example, although what is necessary is to pass only a key and a royalty when already distributed, it may have the above-mentioned contents transportation device, for example, and the contents

may be moved to the 2nd storage from the 1st storage in a transfer of a royalty of contents (duplicate). It is what means that a royalty exists in royalty information on the above 1st, and royalty information on the above 2nd in a license transfer device of above-mentioned this invention, Royalty information on the above 3rd may be a thing showing a royalty not existing, Or royalty information on the above 1st is a thing showing the 1st number of times of usable or available time, Royalty information on the above 2nd is a thing showing the 2nd number of times of usable or available time within the 1st number of times of usable, or available time, Royalty information on the above 3rd may express the 3rd number of times of usable or available time after deducting the 2nd number of times of usable or available time from the 1st number of times of usable or available time.

[0012]In addition, as long as it is the information as which royalty information expresses existence and a range of a royalty for ID which specifies those who have a royalty, for example well also as royalty information, it may be what kind of information. While having the 1st drive and drive of the 2nd that drive the 1st storage and 2nd storage, respectively in a license transfer device of above-mentioned this invention, . The 1st drive and drive of the 2nd access each

the 1st storage and 2nd storage. It has the 1st firmware and 2nd firmware, respectively, The above-mentioned decoding means and the above-mentioned encoding means are constituted in firmware as a complex of the 1st firmware of the above, and the 2nd firmware of the above, While having the title to which only the 1st firmware of the above accesses the 1st storage driven by the 1st drive, it is preferred that it is what has the title to which only the 2nd firmware of the above accesses the 2nd storage driven by the 2nd drive.

[0013]Here "Only the 1st firmware .... it has the title which accesses the 1st storage", and "Only the 2nd firmware .... it has the title which accesses the 2nd storage", For example, from an application program etc. It means being constituted so that the 1st storage or 2nd storage cannot be accessed directly, without making these 1st firmware and the 2nd firmware intervene, When it has such composition, rights of those who have a just right about contents including a case of being as follows will be protected much more certainly.

[0014]Namely, when it is a system which can access a storage directly from an application program temporarily without making firmware intervene, Before transferring a royalty to the 2nd storage from the 1st storage, the 1st encryption secure information that accessed the 1st storage directly and mentioned it above

with an application program is read, and it stores in the 3rd storage. After making such pre-preparations, a royalty is transferred to the 2nd storage from the 1st storage. After the transfer is completed, the 1st encryption secure information before a transfer which accessed the 1st storage directly with an application program again, and carried out the product made from ** to the 3rd storage beforehand is returned to the 1st storage. In this case, it returns to a state before transferring a royalty, and a royalty occurs also in the 2nd storage, and the 1st storage brings about a result by which it infringes on a just right holder's right.

[0015]Then, by making access possible only from firmware as mentioned above, the above unjust generating can be prevented beforehand and a just right holder's right can be protected much more certainly.

[0016]

[Embodiment of the Invention]Hereafter, the embodiment of this invention is described. Here, for intelligibility, a notional embodiment is described first and an embodiment concrete subsequently is described. The lineblock diagram and drawing 2 which drawing 1 shows one embodiment of the license transfer device of this invention are a mimetic diagram for the explanation.

[0017]The 1st storage 10, the drive 20, and the 2nd storage 30 are shown in

drawing 1. All, although the 1st storage 10 and 2nd storage 30 do not ask the kind of the storage, they need to have media ID which specifies the storage. It should be just unique to that storage to such an extent that it can hardly expect this media ID that two storages which do not need to identify certainly the storage of each other of the same kind, and have the same media ID meet.

[0018]A Magnetic-Optical disk drive device in case the 1st drive 10 in which the drive 20 drives the 1st storage 10 in this embodiment, for example, the 1st storage, is MO (magneto-optical disc), When the 2nd drive 30 that drives the 2nd storage 30, for example, the 2nd storage, is a hard disk, an idea is carried out as a complex with the hard disk drive apparatus which drives the hard disk.

[0019]. Become the 1st drive from combination with the software which operates with the microcomputer and its microcomputer. The 1st firmware for accessing the 1st storage driven by the 1st drive is carried, The 2nd firmware for accessing the 1st storage driven by the 2nd drive that becomes the 2nd drive as well as this from combination with the software which operates with a microcomputer and its microcomputer is carried. Here, the firmware as a complex of the 1st firmware and the 2nd firmware shall be idea-carried in the drive 20.

[0020]The 1st storage 10 and 2nd storage 20, Respectively, it has the MID area

11 and 31 which memorizes its own media ID, the secure area 12 and 32 where royalty information and the information about an attribute on contents are stored in addition to this, and the user areas 13 and 33 in which the contents itself are stored. Here, tend to transfer the royalty of contents which the 1st storage 10 has to the 2nd storage 30, therefore here, Media ID of the 1st storage 10, royalty information and other attributes, and contents shall actually be stored in the MID area 11 of the 1st storage 10, the secure area 12, and the user area 13, respectively.

[0021]On the other hand, although media ID of the media 30 of the 2nd storage 30 is stored in the MID area 31 of the 2nd storage 30, The secure area 32 and the user area 33 may be beforehand prepared as a field, or those fields may be generated in the transfer of the royalty of contents.

[0022]Although the decoding means 21 and the encoding means 22 which are explained below, and the contents transportation device 23 are built in the firmware carried in the drive 20 and the application program can start the firmware, It enters into the inside of operation of the firmware, and operation of the firmware is controlled, or it is constituted so that the 1st storage or 2nd storage cannot be accessed directly, without making the firmware intervene.

[0023]That is, the MID area 11 and 31 is area where the lead by firmware is permitted and the light is forbidden, and access to the MID area 11 and 31 is forbidden in principle including the case where application makes firmware intervene. The secure area 12 and 32 and the user areas 13 and 33 are area permitted, and the read/write by firm area application, According to this embodiment, only when firm area is made to intervene, the secure area 12 and 32 and the user areas 13 and 33 can be accessed, and a direct read light cannot be performed. However, it may be the area where direct access by application was permitted about the user areas 13 and 33.

[0024]As for the secure area 12 and 32 and the user areas 13 and 33, about the MID area 11 and 31, it is desirable to be independently provided physically on the nonvolatile storage which is not rewritable. However, in this embodiment, MID area is provided on the 1st storage and the 2nd storage with secure area and user area.

[0025]As shown in drawing 2, the contents stored in the user area 13 of the 1st storage 10 here, It is stored in the form enciphered with the key 1, and that key 1 is the form which was stored in the MID area 11 with the royalty information 41 and which was enciphered with the key 2 which consists of media ID of this 1st

storage 10, and is stored in the secure area 12. Although '1->0' is shown in drawing 2 as the royalty information 41 stored in the secure area 12 here, Meaning that it means that the royalty of the contents exists and, as for '1', '0' does not have a royalty of the contents, it is '1' before the transfer of a royalty and '1->0' means being rewritten by '0' in the case of a royalty transfer. In drawing 2, the secure area 12 and the user area 13 are drawn so that it may extend further on the right, but. This means that two or more contents may be stored in the user area of one storage (here the 1st storage 10), and a key, royalty information, etc. may be stored in the secure area 12 about each contents of these plurality.

[0026]In enciphering the key 1 and the royalty information 41 with the key 2 here, by this drawing 2, it is drawn and are feeling shy as the information with which the key 1 and the royalty information 41 were doubled is enciphered with the key 2, but. That may be right, or the key 1 may be enciphered with the key 2, and the royalty information 41 may be enciphered with the key 2 apart from it. Even if it is which case, what set the both sides of the key 1 enciphered with the key 2 and the royalty information enciphered with the key 2 is called encryption secure information (1st encryption secure information said to this invention) here.

[0027]In the transfer of the royalty of contents by the decoding means 21 of the drive 20 shown in drawing 1. With the key 2 which consists of media ID (1st media ID said to this invention) of the 1st storage 10 memorized in the MID area 11 of the 1st storage 10. The 1st encryption secure information stored in the secure area 12 is decrypted, and the key 1 and the royalty information 41 ('1' which means here that a royalty exists) on a plaintext are taken out by the encryption. Then, the key 1 returned to the plaintext by the decryption and the royalty information 41 ('1' showing a royalty existing) shortly by the encoding means 22 of the drive 20 shown in drawing 1 shortly, It is enciphered with the key 3 which consists of media ID (2nd media ID said to this invention) stored in the MID area 31 of the 2nd storage 30, the 3rd encryption secure information is generated, and it is stored in the secure area 32 of the 2nd storage 30. That the royalty information 42 drawn on the secure area 32 of the 2nd storage 30 in drawing 2 is '0 ->1', Before receiving the transfer of a royalty, what was rewritten by '1' showing a royalty existing is meant by a royalty's not existing, but being '0' and receiving the transfer of a royalty.

[0028]The key 1 which the decrypted royalty information 41 was rewritten by '0' showing a royalty not existing, and was decrypted by the 1st storage 10, The

royalty information showing a royalty not existing is enciphered with the key 2 which consists of media ID of the 1st storage 10, New encryption secure information (3rd secure information said to this invention) is generated, it replaces with the 1st encryption secure information stored in the secure area 12 of the 1st storage 10 till then, and the 3rd newly generated secure information is stored in the secure area 12.

[0029]Or since the royalty of the contents stopped existing in the 1st storage 10, the key 1 is unnecessary, It may replace with generating the 3rd secure information and storing in the secure area 12 of the 1st storage 10, and the key 1 stored in the form enciphered by the secure area 12 may be destroyed. The contents which are stored in the user area 13 of the 1st storage 10 and which were enciphered with the key 1, It is read from the 1st storage 10 by the contents transportation device 23 of the drive 20 shown in drawing 1, and is stored in the user area 33 of the 2nd storage 33 with the state where it was enciphered with the key 1.

[0030]The royalty of contents which the 1st storage 10 owned till then is transferred to the 2nd storage 20 by the above. In the 2nd drive that drives the 2nd storage 20 after it. If there is a read-out demand of these contents from an

application program, the 2nd firmware carried in that 2nd drive, With the key 3 which consists of media ID of the 2nd storage 30 which accessed the 2nd storage 30 and was stored in the MID area 31 of the 2nd storage 30. The encryption secure information stored in the secure area 32 is decrypted, it checks that a royalty exists, the enciphered contents which were stored in the user area 33 with the key 1 are decrypted, and the decrypted contents are returned to an application program.

[0031]On the other hand, after transferring the royalty, by the 1st drive that drives the 1st storage 10. When the read request of the contents which transferred the royalty from an application program occurs temporarily, the 1st firmware carried in the 1st drive, With the key 2 which consists of media ID of the 1st storage 30 which accessed the 1st storage 10 and was stored in the MID area of the 1st storage. It recognizes that a royalty does not exist when the encryption secure information stored in the secure area 12 is decrypted and existence of a royalty is checked, or in the case of the system which destroys the above-mentioned key 1, it recognizes that the key 1 is destroyed or that the contents cannot be decrypted, and the contents cannot be read to an application program -- a purport notice is given. Thus, it can transfer effectively, without

infringing on the right of those who have a right for the royalty of contents about the contents.

[0032]Here, by the above-mentioned embodiment, since it was easy, it explained that royalty information was binary information on '0' showing '1' showing a royalty existing and a royalty not existing, but the number of times of usable may be used as royalty information. For example, the royalty information on the 1st storage 10 before a transfer should be '10' showing the ten number of times of usable, and a part of the number of times of usable, for example, number-of-times of usable 3 batch, may be transferred to the 2nd storage 30. In this case, the royalty information on the 2nd storage 30 is set to '3' showing the three number of times of usable, and '7' showing the seven number of times of usable is returned to the 1st storage 10 as royalty information. With the 1st firmware carried in the 1st firmware carried in the 1st drive whenever it was the use, when the contents were used with the 1st storage 10 or 2nd storage 30, or the 2nd drive. The number of times of usable of the 1st storage 10 or the 2nd storage 30 is subtracted every [1].

[0033]Here, when the royalty of three batches transferred to the 2nd storage 30 has been used up, if the royalty still remains in the 1st storage 10, a part or all of

the royalty can also be again transferred to the 2nd storage in the same procedure as the above. Since it has already moved to the 2nd storage 30, the contents themselves as which it was enciphered in the case of Perilla frutescens (L.) Britton var. crispa (Thunb.) Decne. do not need to move the contents themselves to the 2nd storage 30, and it should merely move only the royalty of the contents to the 2nd storage 30.

[0034]In the example shown in drawing 2, it is considered that the both sides of the key 1 and royalty information are one information, Although the encryption secure information for the 1st storage 10 is generated and the encryption secure information for the 2nd storage 30 is generated by enciphering the information with the key 2 by considering that the both sides of the key 1 and royalty information are one information, and enciphering the information with the key 3, The key 1 and royalty information may be enciphered independently. In that case, what is necessary is to encipher only new royalty information and just to return to the 1st storage 10, since the key 1 is stored in the 1st storage 10 in the already enciphered form in the transfer of a royalty. When dividing the number of times of usable into multiple times and transferring it, in the case of the transfer of the 2nd henceforth. What is necessary is to encipher only the royalty

information showing the number of times of usable which received the transfer with the key 3, and just to write in the secure area 32, since it is already stored in the 2nd storage 30 in the form that the key 1 was enciphered with the key 3.

[0035]Attributes other than the royalty information on the contents, including the name of everything but the key 1 and royalty information, for example, the contents, the last access time of the contents, etc., may also be stored in secure area together, In that case, it may be what may be stored with a plaintext when it is what those attributes do not need to encipher, or those attributes do not need to encipher, or may encipher together with the key 1 or royalty information.

[0036]Although the use count was taken, and it mentioned and was explained as the existence of the royalty as royalty information above, Various information that the existence of a royalty or the usable range is expressed for ID which, in addition to this, expresses the person by whom access was often also as royalty information permitted in available time well also as royalty information can be used as royalty information.

[0037]The appearance perspective view in which drawing 3 shows an example of the computer system by which one embodiment of the license transfer device of this invention is carried, and drawing 4 are the block diagrams showing the

composition of the computer system. This computer system 50 an exterior, As shown in drawing 3, The position on the keyboard 53 which is a handler for performing various kinds of directions to the body part 51 in which CPU, a memory, etc. were built, the image display device 52 which displays a picture on the display screen 52a, and this computer system 50, and the display screen 52a of the image display device 52. It is constituted by the mouse 54 which is a handler for specifying. MO charge mouth 51a loaded with MO(magneto-optical disc) 100 enabling charge and free drawing is shown in the body part 51.

[0038]This computer system 50 an internal configuration top, As shown in drawing 4, As a temporary storing region of CPU55 by which various kinds of programs are executed, the program executed, or data. The memory 56 used, the keyboard interface 57 which delivers data between the keyboards 53, the mouse interface 58 which transmits the data accompanying operation of the mouse 54, the display interface 59 which transmits the data for a display to the image display device 52, It has MO drive 60 which drives MO100 with which it was loaded from MO charge mouth 51 shown in drawing 3, and the hard disk drive 61 which drives the built-in hard disk 62, and they are mutually connected by bus 63, as shown in drawing 4.

[0039]Although the case where the royalty of the contents here stored MO100 in the computer system 50 shown in drawing 3 and drawing 4 is transferred to the hard disk 62 is explained, When simple movement of a royalty or the number of times of usable is set up, about the case where a part of number of times of usable within the number of times of usable is transferred at the first time. With reference to drawing 1 and drawing 2, since it is already explanation settled, below, the number of times of usable transferred at the first time is used up, and the case where the predetermined number of times of usable is transferred again is explained. Although the explanation which referred to drawing 1 and drawing 2 performed explanation notional for an understanding of this invention, it performs more detailed explanation here.

[0040]Drawing 5 is a figure showing the procedure of transferring the royalty of the contents stored in MO100 to the hard disk 62. The application 64 and the drive 20 are shown in this drawing 5. The application 64 expresses the program which directs to be a program which can be operated directly and to transfer the royalty of the contents in MO100 to the hard disk 62 here by the operator of the computer system 50 performed by CPU55. The drive 20 is a complex of MO drive 60 and the hard disk drive 61 which are shown in drawing 4 here. Although

the procedure of transferring the royalty of the contents stored in MO100 to the hard disk 62 is explained below, The royalty which can remain in MO100 and can use for it the contents which it is going to transfer 10 times here remains, and it explains as what transfers 3 times of the royalties of them to the hard disk 62.

[0041]Here, since it is easy, one contents which may be transferred shall mean the contents transferred (or the royalty moved to the hardware 62 by the transfer), when it shall accept and exist and contents are called.

(1) First, towards the application 64 to the drive 20, turn that the transfer origin of contents is MO100 and the transfer place of contents is the hard disk 62 to the drive 20, and specify it (drawing 5 (A)).

[0042](2) If it carries out, the preparations for accessing MO100 and the hard disk 62 will be made, the drive 20 will be the stage in which those preparations were completed, and the drive 20 will report that preparation was completed to the application 64 (drawing 5 (B)).

(3) If it carries out, while sending the password for concealing the information which the drive 20 sends to application in the application 64 to the drive 20 (both sides of MO drive 60 and the hard disk drive 61), Royalty information stored in

the secure area (refer to drawing 1 and drawing 2) of MO100 (here) that in which the royalty information '10' which makes royalty information the information showing the number of times of usable as the above-mentioned premise, and expresses a thing usable 10 times to MO100 now is stored -- carrying out -- the command to read is turned to the drive 20 and published (drawing 5 (C)).

[0043](4) If it carries out, the following processings will be performed within MO drive 60 (refer to drawing 4) which constitutes the drive 20. CPU is carried also in MO drive 60 and here further, The micro program for accessing MO100 with which it was loaded is carried, and the firmware which doubled the hardware and software of these MO drives 60 will perform processing in MO drive 60.

[0044](4-1) Read media ID of MO100 from the MID area (refer to drawing 1 and MID area 11 of drawing 2) of MO100.

(4-2) Read the royalty information enciphered by media ID from the secure area (refer to drawing 1 and secure area 12 of drawing 2) of MO100.

(4-3) Decrypt the read royalty information by media ID.

[0045](4-4) Encode the decrypted royalty information with the password sent from the application 64 in the above-mentioned (3) step.

(4-5) Give the encoded information to the application 64 (drawing 5 (D)).

(5) If it carries out, the application 64 will perform the following processings.

[0046](5-1) Decode with a password the royalty information sent from MO drive 60.

(5-2) '0' showing the ability of the number of times of usable which the decoded royalty information expresses not to use it any more -- check not coming out ('10' which expresses the ten number of times of usable as a premise of explanation is set up here, and it is not '0').

[0047](5-3) Shortly, publish the command which reads the royalty information on the hard disk 62 which is a transfer place of a royalty towards the drive 20 (drawing 5 (E)). As mentioned above, as a premise of explanation, last time, the royalty which can use contents several times is set to the hard disk 62, and the case where the number of times of usable is set to '0' is assumed to it here.

[0048](6) If it carries out, the following processings will be performed in the hard disk drive 61 which drives the hard disk 62. The hard disk drive 61 is also equipped with CPU or the micro program, and processing in the hard disk drive 61 as well as the processing in MO drive 60 is performed by the firmware as a complex of these hardwares and software.

[0049](6-1) Read media ID of the hard disk 62 from the MID area (refer to

drawing 1 and MID area 31 of drawing 2) of the hard disk 62.

(6-2) Read the royalty information enciphered by media ID of the hard disk 62 from the secure area (refer to drawing 1 and secure area 32 of drawing 2) of the hard disk 62.

[0050](6-3) Decrypt the read royalty information by media ID of the hard disk 62.

(6-4) Encode the decrypted royalty information with the password sent from the application 64 in the above-mentioned step of (3). (6-5) Give the encoded royalty information to the application 64 (drawing 5 (F)).

[0051](7) If it carries out, the application 64 will perform the following processings.

(7-1) Decode with a password the royalty information sent from the hard disk drive 61.

(7-2) Check that the decoded royalty information expresses the number of times '0' of usable.

[0052]When the number of times of usable expresses not '0' but the still usable thing, it displays on the still usable purport display screen 52a (refer to drawing 3), that is notified to an operator, and processing is interrupted for this embodiment in this stage. Here, as a premise of explanation, the number of

times of usable is '0', and he follows it to the following processings further in this case.

[0053](7-3) Encode with a password the information (new frequency information is called) showing the number of times (it is based on the premise of explanation here and is 3 times) of usable newly set as the hard disk 62, and send to the drive 20 (both sides of MO drive 60 and the hard disk drive 61) (drawing 5 (G)).

(8) In MO drive 60, the following processings are performed in response to this new frequency information.

[0054](8-1) Read media ID of MO100.

(8-2) Read the royalty information in the state where it was enciphered by media ID of MO100 stored in the secure area of MO100.

(8-3) Decrypt the enciphered royalty information by media ID of MO100, and take out the number of times '10' of usable.

[0055](8-4) Decode the new frequency information which has been sent from the application 64 and which was encoded with the password with the password sent at the above-mentioned step of (3), and take out the number of times '3' of usable.

(8-5) Deduct the number of times '3' of usable which it is going to transfer to the

hard disk 62 from the number of times '10' of usable stored in MO100 till then, and obtain the new number of times '7' of usable.

(8-6) Encipher the new royalty information showing the new number of times '7' of usable by media ID of MO100.

[0056](8-7) Overwrite the royalty information showing the number of times '10' of usable stored in MO100 till then in the enciphered new royalty information. Thereby, the number of times '7' of usable is set as MO100.

(9) On the other hand by the hard disk drive 61, the following processings are performed in response to the new frequency information sent at the above-mentioned step of (7-3).

[0057](9-1) Read media ID of the hard disk 62.

(9-2) Decode the new frequency information which has been sent from the application 64 and which was encoded with the password with the password sent at the above-mentioned step of (3), and take out the number of times '3' of usable.

(9-3) Encipher the new royalty information showing the number of times '3' of usable taken out by the decoding by media ID of the hard disk 62.

[0058](9-4) Overwrite the royalty information showing the number of times '0' of

usable stored in the hard disk 62 in the enciphered new royalty information. Thereby, the number of times '3' of usable is set to the hard disk 62.

(10) The application 64 is notified that processing of the above royalty transfer was completed from the drive 20.

[0059]The transfer (here transfer of a part of royalty) of the royalty of contents is performed as mentioned above. Although reference is not made in explanation of the more than which referred to drawing 5 about movement of the key for decrypting the contents themselves and the enciphered contents from MO100 to the hard disk 62, as mentioned above, Here, the key for explaining the case of setting out of the number of times of usable of contents for the second time, therefore decrypting the contents themselves and it is premised on the hard disk 62 already being passed at the time of a first-time transfer. The contents themselves are moved to the hard disk 62 from MO100 with the form enciphered at the time of a first-time transfer (duplicate), and the above-mentioned explanation, The key is premised on being enciphered independently of royalty information by each media ID, and being stored in each secure area.

[0060]In the embodiment described with reference to drawing 5, as mentioned above, are advancing processing of the transfer of the royalty of contents,

performing communication with various applications 64 and drives 20, but. Replace with such contents transfer processing and from the application 64. The transfer origin of the contents which are going to transfer the royalty, and the royalty of the contents (here MO100), a transfer place (here hard disk 62) -- and it is going to transfer. Specify the number of times of a royalty and he leaves processing to the drive 20 (here, they are the both sides of MO drive 60 and the hard disk drive 61) after that, In the drive 20, the above-mentioned transfer processing is performed independently [the application 64], transfer processing was not normally performed by the stage which transfer processing ended, and a certain inconvenience (for example, only the number of times of usable of less than the number of times of usable that had the transfer specified by MO100 remained.) Or only at the time [set / the number of times of usable which received the transfer in the hard disk 62 at last time / to '0' / yet], it may constitute so that it may report to the application 64.

[0061]Although MO drive 60 and the hard disk drive 61 share the above-mentioned transfer processing 60 and it is performed by the above-mentioned explanation, One of these MO drives and the hard disk drives 61 may be only for access, and it may constitute so that the above-mentioned

transfer processing may be chiefly performed by another side. The figure and drawing 7 which drawing 6 shows an example of the computer network in which one embodiment of the license transfer device of this invention was included, It is a figure showing the procedure at the time of transferring the royalty of contents to another computer system from a certain computer system which constitutes the computer network.

[0062]Here two sets of the computer system 70 for contents managing and the computer systems 80 and 90 of the side which uses contents are shown, and these three sets of the computer systems 70, 80, and 90 are mutually connected via the communication line 200. Each computer systems 70, 80, and 90 are provided with the composition as the computer system 50 shown in drawing 3 with same each. Namely, each computer systems 70, 80, and 90, It has each body parts 71, 81, and 91, each image display devices 72, 82, and 92, each keyboards 73, 83, and 93, and each mice 74, 84, and 94, and each computer systems 70, 80, and 90 are further provided with the internal configuration as the internal configuration shown in drawing 4 with same each. Detailed explanation is omitted.

[0063]Here, the computer system 70 for contents managing shall be installed in

the head office of a certain company, and the computer systems 80 and 90 of the side which uses contents shall be installed in each branch office of the company. Below, since explanation is easy, a head office and the computer systems 70, 80, and 90 installed in each branch office are called the head office 70, the branch office 80, and the branch office 90 as they are.

[0064]Here, the license for all the branch offices of various kinds of contents is purchased, and a license is distributed to each branch office from the head office in a head office, and it is assumed that the license for all the branch offices is managed in the head office. That is, even if it is the same contents, a required number of royalties are purchased in a head office, and the royalty is distributed to the branch office which needs the contents here. A required number about the same contents here of royalties, Only a number as occasion demands purchases the royalty of the same contents the same with carrying out two or more volume (for example, three volumes) purchase of the same book instead of what means the use count of the contents, and the number of purchased royalties are meant here. A number of the remaining numbers that distributed the royalty from the number of the purchased royalties to the branch office about each contents in the head office are managed, and at each branch office. The

chisel is managed [whether two or more royalties about the same contents are unnecessary, and a royalty exists in its branch office about each contents, and]. At a head office and each branch office, the royalty information on much contents is managed and the list of the royalty information on the contents of these large number is called 'granted information' here.

[0065]Here, the royalty of various contents is already transferred from the head office 70 to each branch offices 80 and 90, Furthermore, the royalty of a certain contents shall be transferred from the head office 70 this time to a certain branch office (here, it is considered as the branch office 80) (here). The scene of calling 'new contents' the contents which are trying to perform the new transfer of a royalty and of transferring the royalty of the new contents to the branch office 80 here is explained. Here, the royalty of new contents shall be transferred to the hard disk of the branch office 80 from the hard disk of the head office 70.

[0066](1) the royalty of new contents is first transferred towards the branch office 80 from the head office 70 -- carry out purport connection (drawing 7 (A)).

(2) If the hard disk of the branch office 80 will be made into a preparatory state in response to the connection at the branch office 80 if it carries out, and preparation of access is completed, what preparation was able to carry out to the

head office 70 will be reported (drawing 7 (B)).

[0067](3) The password for concealing the information sent from the branch office 80 in the head office 70, if it carries out is sent out to the branch office 80, A command is published [sending the granted information (list showing the existence of the royalty of two or more contents of each of information) furthermore stored in the secure area of the hard disk of the branch office 80, and] (drawing 7 (C)).

(4) Perform the following processings in response to this command at the branch office 80.

[0068](4-1) Read media ID of the hard disk of the branch office 80.

(4-2) Read the granted information enciphered by media ID of the hard disk from the secure area of the hard disk of the branch office 80.

(4-3) Decrypt by media ID which read the read granted information.

(4-4) Encode media ID of the hard disk of the branch office 80 further with the decrypted granted information with the password sent from the head office 70 in the above-mentioned step of (3).

[0069](4-5) Send the granted information and media ID which were encoded to the head office 70 (drawing 7 (D)).

(5) If it carries out, the following processings will be performed in the head office 70.

(5-1) Decode with a password the granted information and media ID which have been sent from the branch office 80.

[0070](5-2) Check that the royalty about the new contents which are trying to move a royalty to the branch office 80 from now on does not exist in the branch office 80, seeing the decoded granted information. This is for avoiding carrying out duplication setting out of the royalty of the same contents to the same branch office.

(5-3) Read media ID of the hard disk of the head office 70.

[0071](5-4) Read the key for decrypting the granted information enciphered by media ID of the hard disk, and the contents which were similarly enciphered by the media ID and which are going to permit the royalty from the secure area of the hard disk of the head office 70.

(5-5) Decrypt the read granted information and key by read media ID.

[0072](5-6) Check that the royalty about the contents (new contents) which are newly going to transfer the royalty to the branch office 80 has the remainder with reference to the decrypted granted information. When there is no remainder, it

will tell the purport branch office 80 which cannot license the new contents, but it is assumed here that the royalty of the new contents remains in the head office 70.

[0073](5-7) Rewrite the information showing the royalty of new contents in the granted information of the branch office 80 decoded at the above-mentioned step of (5-1) from 'with no royalty' to 'those with a royalty'.

(5-8) Encode the rewritten granted information and the both sides of a key with a password.

[0074](5-9) Read the enciphered new contents from the user area of the hard disk of the head office 70.

(5-10) Send the encoded granted information, a key, and the new contents enciphered to the branch office 80 (drawing 7 (E)).

(5-11) When only 1 subtracts the information about the number of the royalties about the new contents which permitted the royalty this time to the branch office 80 in the granted information of the head office 70 decrypted at the above-mentioned step of (5-5) in the head office 70, update to new granted information.

[0075](5-12) Encipher the new granted information updated by making it such by

media ID of the hard disk of the head office 70.

(5-13) Replace with and store the enciphered new granted information in the granted information before updating stored there till then in the secure area of the hard disk of the head office 70.

[0076](6) At the branch office 80, receive the encoded granted information and the key which have been sent at the above-mentioned step of (5-10), and the enciphered new contents, and perform the following processings.

(6-1) While it had been enciphered, store the received new contents in the user area of your own (branch office 80) hard disk.

[0077](6-2) Decode the granted information and the key which were received with the password sent at the above-mentioned step (3).

(6-3) Read media ID of your own (branch office 80) hard disk.

(6-4) Encipher the granted information and the key which were decoded with the password by the read media ID.

[0078](6-5) As the granted information stored in the secure area of its own (branch office 80) hard disk till then in the granted information and key which were enciphered is rewritten, store it. The royalty of the new contents is transferred to the branch office 80 from the head office 70 by the above.

[0079]As shown in each above embodiment, in the network which connected two or more computers into one device which consists of one computer etc., the license transfer device of this invention is realizable.

[0080]

[Effect of the Invention]As explained above, according to this invention, the contents can be reproduced or distributed, without infringing on the right of those who have a right about contents.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a lineblock diagram showing one embodiment of the license transfer device of this invention.

[Drawing 2]It is a mimetic diagram for explanation of the license transfer device shown in drawing 1.

[Drawing 3]It is an appearance perspective view showing an example of the computer system by which one embodiment of the license transfer device of this invention is carried.

[Drawing 4]It is a block diagram showing the composition of the computer system which shows drawing 3 appearance.

[Drawing 5]It is a figure showing the procedure of transferring the royalty of the

contents stored in MO to a hard disk.

[Drawing 6]It is a figure showing an example of the computer network in which one embodiment of the license transfer device of this invention was included.

[Drawing 7]It is a figure showing the procedure at the time of transferring the royalty of contents to another computer system from the computer system which constitutes the computer network shown in drawing 6.

[Description of Notations]

10 The 1st storage

11 MID area

12 Secure area

13 User area

20 Drive

21 Decoding means

22 Encoding means

23 Contents transportation device

30 The 2nd storage

31 MID area

32 Secure area

33 User area

41 and 42 Royalty information

50 Computer system

51 Body part

51a MO charge mouth

52 Image display device

52a Display screen

53 Keyboard

54 Mouse

55 CPU

56 Memory

57 Keyboard interface

58 Mouse interface

59 Display interface

60 MO drive

61 Hard disk drive

62 Hard disk

70, 80, and 90 Computer system

71, 81, and 91 Body part

72, 82, and 92 Image display device

73, 83, and 93 Keyboard

74, 84, and 94 Mouse

100 MO (optical magnetism DISUKKU)

200 Communication line